

What is Claimed:

1. A method for calculating a greatest common divisor of a first binary integer, U, and a second binary integer, V, the method comprising the steps of:

a) selecting 2M most significant bits of U as a first value U_{2M} and selecting 2M corresponding bits of V as a second value V_{2M} , dividing U_{2M} by V_{2M} and storing an integer portion of the result as a value Q;

b) determining a value T as U minus the quantity Q times V;

c) if T is less than zero, applying a correction term to Q to obtain a corrected value Q' and assigning the new value for T as U minus the quantity Q' times V;

d) assigning V to U and T to V; and

e) repeating steps a) through d) until V equals zero, whereby the value remaining in U is the greatest common divisor of the first and second binary integers.

2. A method according to claim 1, wherein:

step c) includes the step of selecting 2M most significant non-zero bits of T to define a value T_{2M} , wherein the step of applying the correction term is given by the equation:

$$Q' = Q - (\lfloor T_{2M} / V_{2M} \rfloor + 1); \text{ and}$$

step c) further includes the step of calculating Q'', a further corrected value for Q, as the greatest integer less than the quantity U divided by V if the new value of T is less than zero.

1 *Sub*
2 *Pat*
3 3. A method according to claim 1, wherein the first binary integer,
4 U, has a most significant non-zero bit at bit-position B1 and the second binary integer,
5 V, has a most significant non-zero bit at bit-position B2, where B1 and B2 are integers
6 and B1 is greater than B2, the method further including the steps of:

7 subtracting B2 from B1 to obtain a difference value D;

8 comparing D to a predetermined threshold value wherein steps a)
9 through d) are performed only if D is greater than a predetermined threshold value;

10 if D is not greater than the predetermined threshold, then, before step e)
11 performing the steps of:

12 determining values X and Y such that U_{2M} times X plus V_{2M} times
13 Y is less than 2^M ;

14 assigning a new value to U as U times X plus Y times V; and

15 switching the values of U and V.

1 4. A method according to claim 3, wherein the step of determining
2 values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M , includes the
3 step of invoking a further GCD routine.

4 5. A method according to claim 4, wherein $2M$ equals 32 and the
5 further GCD routine is a Euclid routine having a modified termination condition.

6 6. A method according to claim 4, wherein $2M$ equals 64 and the
7 further GCD routine is a Lehmer routine having a modified termination condition.

8 7. A method according to claim 1, further including a method for
9 calculating a value V^{-1} being the inverse of V modulo U, wherein:

Sub
3 step a) further includes the steps of assigning a value of zero to a
4 temporary variable U2 and assigning a value of one to a temporary variable V2; and

5 step d) further includes the steps of determining a value T2 as U2 minus
6 Q times V2, assigning the value in V2 to U2 and assigning the value T2 to V2;

7 whereby, at step e) when V equals zero, the value of U2 is V^{-1} .

1 8. A method according to claim 3, further including a method for
2 calculating a value V^{-1} being the inverse of V modulo U, wherein:

3 step a) further includes the steps of assigning a value of zero to a
4 temporary variable U2 and assigning a value of one to a temporary variable V2; and

5 step d) further includes the steps of determining a value T2 as U2 minus
6 Q times V2, assigning the value in V2 to U2 and assigning the value T2 to V2;

7 the step of assigning a new value to U as U times X plus Y times V,
8 further includes the step of determining the value T2 as X times U2 plus Y times V2;
9 and

10 the step of switching the values of U and V further includes the step of
11 assigning the value of V2 to U2 and assigning the value T2 to V2;

12 whereby, at step e), when V equals zero, the value of U2 is V^{-1} .

1 9. A method for defining a Finite field that includes encryption keys
2 for an encryption algorithm, comprising the steps of:

3 a) selecting a first binary integer value, P, having a number of bits such
4 that the Finite field defined as values ranging between zero and the first value are
5 sufficient for the encryption algorithm to be secure;

6 b) determining if P is a prime number, comprising the steps of:

097643-01704

7 *Sub*
8 *ai.* calculating a greatest common divisor of P, and a second binary integer,
V, wherein V is a product of predetermined prime numbers, including the steps of:

9 b1) assigning P to a temporary variable U;

10 b2) selecting 2M most significant non-zero bits of U as a first
11 value U_{2M} and selecting 2M corresponding bits of V as a second value V_{2M} ,
12 dividing U_{2M} by V_{2M} and storing an integer portion of the result as a value Q;

13 b3) determining a value T as U minus the quantity Q times V;

14 b4) if T is less than zero, applying a correction term to Q to
15 obtain a corrected value Q' and assigning the new value for T as U minus the
16 quantity Q' times V;

17 b5) assigning V to U and T to V; and

18 b6) repeating steps a) through e) until V equals zero, whereby the
19 value remaining in U is the greatest common divisor of the first and second
20 binary integers;

21 c) if U is greater than one, selecting an other value for P and repeating
22 steps b) through c) until U is equal to one;

23 d) when U is equal to one after step c), passing P to a probabilistic
24 primality testing routine to determine if P is prime;

25 whereby when P is prime, the integers from 0 to P define the Finite
26 field.

1 10. A method according to claim 9, wherein:

0976433-044704

2 *Sub* step b4) includes the step of selecting 2M most significant non-zero bits
3 of T to define a value T_{2M} , wherein the step of applying the correction term is given
4 by the equation:

5
$$Q' = Q - (\lfloor T_{2M} / V_{2M} \rfloor + 1); \text{ and}$$

6 step c) further includes the step of calculating Q'' , a further corrected
7 value for Q, as the greatest integer less than the quantity U divided by V if the new
8 value of T is less than zero.

1 11. A method according to claim 10, wherein the first binary integer,
2 U, has a most significant non-zero bit at bit-position B1 and the second binary integer,
3 V, has a most significant non-zero bit at bit-position B2, where B1 and B2 are integers
4 and B1 is greater than B2, the method further including the steps of:

5 subtracting B2 from B1 to obtain a difference value D;

6 comparing D to a predetermined threshold value wherein steps a)
7 through d) are performed only if D is greater than a predetermined threshold value;

8 if D is not greater than the predetermined threshold, then, before step e)
9 performing the steps of:

10 determining values X and Y such that U_{2M} times X plus V_{2M} times
11 Y is less than 2^M ;

12 assigning a new value to U as U times X plus Y times V; and

13 switching the values of U and V; and

14 after step e) if U is greater than 1, further processing U to remove
15 spurious factors.

05764E13.01704

*Sub
all*

1 12. A method according to claim 11, wherein the step of determining
2 values X and Y such that U_{2M} times X plus V_{2M} times Y is less than 2^M , includes the
3 step of invoking a further GCD routine.

1 13. A method according to claim 12, wherein 2M equals 32 and the
2 further GCD routine is a Euclid routine having a modified termination condition.

1 14. A method according to claim 12, wherein 2M equals 64 and the
2 further GCD routine is a Lehmer GCD routine having a modified termination
3 condition.

1 15. A method for identifying an encryption value in a Finite field, F_P ,
2 where P is a prime number, based on a private key PV and a received public key PB,
3 comprising the steps of:

4 determining a mathematical inverse of PB modulo P by performing the
5 steps of:

6 a) assigning P to a temporary variable U and assigning PB to a
7 temporary variable V and assigning a value of zero to a temporary variable U2
8 and assigning a value of one to a temporary variable V2;

9 b) selecting 2M most significant bits of U as a first value U_{2M} and
10 selecting 2M most significant bits of V as a second value V_{2M} , dividing U_{2M} by
11 V_{2M} and storing an integer portion of the result as a value Q;

12 c) determining a value T as U minus the quantity Q times V;

13 d) if T is less than zero, applying a correction term to Q to obtain
14 a corrected value Q' and assigning the new value for T as U minus the quantity
15 Q' times V;

0976423-014704

*Sub
a1*

16 e) determining a value T2 as U2 minus Q times V2, assigning the
17 value in V2 to U2, assigning the value T2 to U2, assigning V to U and T to V;
18 and

19 f) repeating steps a) through e) until V equals zero, whereby the
20 value remaining in U2 is the mathematical inverse of PB; and

21 dividing PV by PB modulo P by multiplying PV times the mathematical
22 inverse of PB, wherein the result is the encryption value.

1 16. A method according to claim 15, wherein:

2 step d) includes the step of selecting 2M most significant bits of T to
3 define a value T_M , wherein the step of applying the correction term is given by the
4 equation:

$$5 \quad Q' = Q - (\lfloor T_{2M} / V_{2M} \rfloor + 1); \text{ and}$$

6 step d) further includes the step of calculating Q'' , a further corrected
7 value for Q, as the greatest integer less than the quantity U divided by V if the new
8 value of T is less than zero.

1 17. A method according to claim 15, wherein the variable U has a
2 most significant bit at bit-position B1 and the variable V has a most significant bit at
3 bit-position B2, where B1 and B2 are integers and B1 is greater than B2, the method
4 further including the steps of:

5 subtracting B2 from B1 to obtain a difference value D;

6 comparing D to a predetermined threshold value wherein steps a)
7 through d) are performed only if D is greater than a predetermined threshold value;

8 if D is not greater than the predetermined threshold, then, before step e)
9 performing the steps of:

0976123-01104

1 20. A method according to claim 17, wherein 2M equals 64 and the
2 further GCD routine is a Lehmer routine having a modified termination condition.